INTERNAL AUDIT

CONTROLS EVALUATION

CAD SYSTEM

December 20, 2004

Roanoke City Council Audit Committee
Roanoke, Virginia

We have completed an audit of the Computer Aided Dispatch system (CAD) and E-911 Center. We performed this audit in accordance with generally accepted government auditing standards.

BACKGROUND

The E-911 Center operates 24 hours a day, 365 days a year. The Center answers all 911 calls originating from within the City of Roanoke and also serves as the backup call center for Roanoke County. Phone calls to certain other city phone numbers after normal business hours are also routed to the E-911 Center. This includes calls to Parks and Recreation, the Child Abuse Hotline, the Information Desk, and Public Works.

In 2003, the E-911 Center processed 147,426 calls for Police and 21,370 calls for Fire/EMS. As of September 7, 2004, the E-911 Center had processed 104,079 calls for Police and 15,062 for Fire/EMS. These totals do not include those calls for other city services answered by the E-911 Center after hours. When such calls are received, the E-911 staff enters the caller's request and contact information into the City's service request system. If the request requires an immediate response, the E-911 staff contacts the on-call person for the appropriate department. All calls to the Child Abuse Hotline are immediately conveyed to the on-call social worker.

The E-911 Center has 41 employees that staff three 8-hour shifts. The staff includes a Superintendent, a Systems Administrator, a Communications Coordinator, four supervisors, and 34 dispatchers. All dispatchers are required to complete a one year probationary/training period. Each dispatcher must become certified in CPR (Cardio Pulmonary Resuscitation), EMD (Emergency Medical Dispatch), and VCIN (Virginia Criminal Information Network) within this first year. The dispatchers must also meet ongoing educational requirements in order to maintain their certifications.

The E-911 Center has been using Motorola's Premier Computer Aided Dispatch, or CAD, system to route calls and dispatch public safety personnel since September 1999. When a 911 call is answered by the system, the caller's name, address, and location instantly appear on the dispatcher's screen. If the call is from a cellular phone, the tower site, cellular company, and cell number are the only items of information that appear on the screen. The callback cellular telephone number is only provided on registered

telephones. Cellular callers with Phase II (telephones with location technology) can be integrated by the dispatcher to obtain the location of the cellular caller. This information is then displayed to the dispatcher on the Computer-Assisted-Dispatching map. The dispatcher then has to determine the address of the caller based on the map information. Once the dispatcher verifies that emergency assistance is needed, he or she confirms the caller's information and corrects it in the CAD system if necessary. The dispatcher then enters the incident type and a basic description of the incident into the CAD system. The CAD system assigns a priority level to the call based on the incident type. The dispatcher sends the call on to another workstation for routing so that he or she can take another call. There are two routing work stations in the E-911 Center, one for fire and rescue service calls and one for police assistance calls.

In the case of fire and rescue, the CAD system has been programmed to automatically identify the closest available station relative to the incident and the system will display the station onto the screen for the dispatcher. The dispatcher will release the dispatch and also broadcast the call over the radio system in case an engine crew is not at the station. The call prints out at the station and the station acknowledges receiving the call.

Police units are continuously monitored by the CAD system as to their availability to take calls. The dispatcher reviews the calls for police assistance and filters duplicate calls before releasing them to the CAD system queue. Once in queue, the calls for police assistance are automatically dispatched to the first available police unit. If units are not available, the call will remain in queue until the call times-out, based upon its priority level. The priority is assigned based on the nature of the call and may not require an immediate response. Low priority calls are held until a unit becomes available, especially if a shift change is in progress. Once the time limit for holding a call is reached, the dispatcher will broadcast the call over the radio system based on its priority. For a lower priority call, the dispatcher will contact a police supervisor to determine the proper action for the call. Police units will then log themselves into the system if the call takes precedence over whatever they are currently doing. If an excessive number of calls remain in the queue, the police supervisor may instruct units to become available. The response time for the unit is measured from the point the call is accepted by a unit.

The 911 call data resides on a tandem server located in the E-911 Center. The call data is active on the tandem server for six months before it is purged from the system. On a continual basis, the 911 call data is replicated to a data analysis server from where the Police and Fire departments can import call data into their respective records systems.

PURPOSE

The purpose of this audit was to evaluate the system of internal controls applicable to the following areas:

- Dispatch quality control
- Staff training and certification

- System access
- Backup procedures
- Data transfer utility

SCOPE

The audit will focus on the system of internal controls in place as of June 1, 2004. We tested data generated between July 1, 2003 and June 1, 2004.

METHODOLOGY

We gained an understanding of the CAD system and associated processes by reviewing system manuals, policies and procedures manuals, and by observing and interviewing E-911 Center personnel. We documented our understanding of the system of controls in place with process outlines. Based on this understanding, we documented the system of internal controls and developed a test program to evaluate the operation and effectiveness of significant controls. Our test plan included reviewing documentation supporting staff training, staff certification, and quality control reviews. We performed tests to determine if the backup procedures were adequate. We also performed various data analyses to verify that the 911 call records are replicated to the data analysis server. We selected a sample of users to the CAD system and reviewed their access rights. Access lists were reviewed for the CAD and related systems.

RESULTS

Our test work indicated that quality control reviews were being performed and that 911 call records were replicated to the data analysis database. We identified other minor issues that were discussed with management for their review and consideration.

Finding 01: User IDs

We reviewed the existing user IDs and their related access rights to the data analysis server, where the 911 dispatch data resides for import into the fire and police records systems. We noted that there were two user IDs with “administrative rights” to the database which allow the user to add, modify, and delete data. One of the user IDs was used by the application vendor and Technology staff to set up the database and to access the database as needed. The other user ID was used by a Police department employee and Fire department employee to enable them to analyze data into their respective records systems.

Sharing passwords reduces the ability of a system administrator to properly control access by individuals and to monitor activity by individuals. Providing users with the ability to delete and modify data increases the risk that historical data will not be complete and reliable. Control Objectives for Information Technology Standards set by the Information Systems Audit and Control Association state that access rights should be

limited to a minimum number of vendor staff and that the access should be the least needed. Based on our discussions with the police and fire employees involved, we believe they were not aware that they had the ability to modify or delete data.

Agreed Upon Action 01: User IDs

The Department of Technology will review the vendor's need for access to the database and establish a unique user ID. The vendor will reset the associated password with its ID, so it will only be known to the vendor. The vendor will be provided with the minimum access rights necessary to perform required work. The users in the Police and Fire departments will share a user ID limited to reading data only. The Department of Technology employees will establish unique user IDs for themselves. Existing user IDs with administrative rights will be deleted, if possible, or the associated access rights will be modified to be read only.

CONCLUSION

Based on the results of our audit work, we believe that quality control processes, backup procedures, data transfer utilities, staff training, and certification have been well controlled. We believe that controls over system access could be strengthened by taking the actions noted.

We would like to thank the management and staff of the E-911 Center and the Department of Technology for their assistance throughout the audit.

Pamela C. Mosdell, CISA, CIA
Information Systems Auditor

Michael J. Tuck, CPA, CGAP
Assistant Municipal Auditor

Drew Harmon, CPA, CIA
Municipal Auditor